Otros Conceptos: FEDERACION / SSO

**¿Qué es federar identidades?**

**Federación** de identidad: es la vinculación de por ejemplo mi identidad en un IdentityServerA contra otra identidad también de mi propiedad, en **otro IdentityProviderB**. Para ello es necesario que **ambos IdentityProviders consensúen** los mecanismos mutuos de confianza **en todos los escenarios del journey del usuario en ambos serviceProviders**.

Esta funcionalidad es utilizada para hacer sinergia entre serviceProviders pero no necesariamente implica un SSO entre ambos. La mayoría de los casos pueden entenderse si pensamos en los escenarios de pago: el serviceProviderA confía, delega en los serviceProviderB, serviceProviderC, serviceProviderD,  la **autenticación de la identidad** para realizar un pago. Esto implica:

* + ServiceProviderA es responsable de la seguridad y autenticación e2e
  + ServiceProviderA asume como suficiente la autenticación que llevan a cabo serviceProviderB, serviceProviderC y serviceProviderD.
  + las credenciales del usuario para ServiceProviderA no son compartidas con los otros serviceProviders
  + las credenciales del usuario en los serviceProvidersB, C y D no son compartidas con serviceProviderA.

el usuario final controla y gobierna sus credenciales para los serviceProviders independientemente y **no existe sincronización alguna entre éstas**.

**¿Qué es SSO?**

SSO, acrónimo de **Single** Sign On describe el escenario donde un conjunto de aplicaciones “miembro” del SSO compartirán la sesión con un único Sign On.

El ejemplo clásico es nuestra cuenta de Google, donde podemos utilizar diferentes aplicaciones con nuestro “usuario de Google”.

Es importante entender que al definir un escenario SSO estamos definiendo:

* una **única** sesión para todas las aplicaciones miembro
* un **único** signOn y signOff
* una credencial **única**

Cabe destacar que con la digitalización de los servicios vemos actualmente gran cantidad de escenarios donde estas features están incorrectamente implementadas, lo que ofrece puntos de vulnerabilidad a la seguridad de las credenciales.

Por eso, es necesario que Telecom establezca lineamientos claros, simples y sustentables como requisitos de compliance para toda solución que interactúe con nuestro ecosistema.

No debe confundirse con **recordar** mi usuario. En este escenario, **serviceProvider** y **IdentityProvider** acuerdan “recordar” las credenciales de un usuario para evitar solicitarle el login manual al vencer la sesión o hacer logout.